Secure Sharing of Electronic Health Records to Ensure Privacy

[1]Vinayak K B, [2]Prof. H R Shashidhar
[1]M.Tech Scholar, [2]Assistant Professor
RNS Institute of Technology, Bangalore, Karnataka, India
[1]vinu.kb89@gmail.com, [2]shashi_dhara@yahoo.com

***Abstract* - Electronic Health Records (EHR) is the medical records use to maintain by the hospitals electronically instead of paper. Generally Hospitals document, manage and update the status of patients admitted. As the patient's records are very sensitive, in order to provide a security a proper security method should be followed by the hospital authorities. At the same time, Chain of hospitals uses to share electronic health records with other hospitals. While sharing, there might be chances of record alteration and hackers attack. In our paper we propose an health care centric framework and suite of mechanisms for data access control of electronic health record stored in server. To achieve a secured data access control, Multi Authority Attribute based Encryption is used where it provides security for attributes (such as patients, doctor, research and scholar) of a EHRs and it allows patients and doctor to manage EHR and to share the records with other hospitals.**

***Keywords* - Electronic Health Records, Attribute Based Encryption, Healthcare, Server**

I. INTRODUCTION

Healthcare ecosystem consists of the healthcare providers such as doctors, physicians, specialists etc and payers such as health insurance companies, pharmaceutical companies, IT solutions and services firms, and the patients. The process of provisioning healthcare involves massive healthcare data which exists in different forms (structured or unstructured) on disparate data sources (such as relational databases, file servers, etc.) and in different formats.

When a patient is admitted to a hospital, his/her information is entered into Electronic Health Record (EHR) systems. Physicians diagnose the patient and the diagnostic information (from medical devices such as CT scanners, MRI scanners, etc) is stored in EHR systems. In the diagnosis process, the doctors retrieve the health information of patients and analyze it to diagnose the illness. Doctors can take expert advice by sharing the information with consulting specialists.

The Server can provide several benefits to all the stakeholders in the healthcare ecosystem through systems such as Health Information Management System (HIMS), Laboratory Information System (LIS), Radiology Information System (RIS), Pharmacy Information System (PIS), etc. With EHR systems hospitals don't need to spend a significant portion of their budgets on IT infrastructure. service providers provide on-demand provisioning of hard ware resources with pay-per-use pricing models. Thus hospitals using server based EHR systems can save on upfront capital investments on maintenance of paper based records.

In modern healthcare domain, electronic health records (EHRs) have been widely adopted to enable healthcare providers, insurance companies and patients to create, manage and access patients' healthcare information from anywhere and at any time. Typically, a patient may have many different healthcare providers including primary care physicians, specialists, therapists, and miscellaneous medical practitioners. Besides, a patient may have different types of insurances, such as medical insurance, dental insurance and vision insurance, from different healthcare insurance companies.

As system is based on client and server architecture, Server will be maintaining the all records of patients and each health care provider will be having server to maintain their records As a result, a patient's EHRs can be found scattered throughout the entire healthcare sector. From the clinical perspective, in order to deliver quality patient care, it is critical to access the integrated patient care information that is often collected at the point of care to ensure the freshness of time-sensitive data.

In some emergency healthcare situations, immediate exchange of patient's EHRs is crucial to save lives. However, in current healthcare settings, healthcare providers mostly establish and maintain their own electronic medical record (EMR) systems for storing and managing EHRs. This kind of self-managed data centers are boon for healthcare providers.

A MA-ABE based approach for secure sharing Electronic Health Record (EHR) systems to ensure privacy. Healthcare Server environments provide several benefits to all the stakeholders in the healthcare ecosystem (patients, providers, payers, etc.). Lack of security and privacy has been a major obstacle in the exchange of healthcare data between different stakeholders. The Multi Authority concept is used for abstracting the data from the EHR based on the users authority. In multi authority technique, all the users are assigned an authority and based on this authority data from the EHR is displayed to the user.

II. RELATED WORK

Patient Health Record (PHR)systems are patient-facing portals that contain patient health information and allow patients to interact with the health system. The Famous Markle Foundation defines a PHR as "a set of tools that allow patients to access and coordinate their lifelong health information and make appropriate parts of it available to those who need it."

All these systems provide repositories and portals to access data. However, each tool serves a different purpose. Ultimately, the value of these systems is in providing the data and user interfaces to enable other applications and functionalities. It is important to note that the degree of information provided in an EMR, EHR or PHR is a function of the clinical information systems that populate the patient record (e.g., lab, diagnostic imaging, pharmacy, structured electronic charting,clinical decision support). Some of Disadvantages of PHR System are:

- The only real disadvantage to PHR is that there may be a lack of privacy involved.
- It is estimated that a total of 150 people can have access to PHR records at a time. This can lead to altered information and even lack of privacy for patients and their families.
- As Hospitals will be Geographical distributed, each hospital cannot access the EHRs of other hospitals server.

III. PROPOSED WORK

In the proposed system, Multi-Authority Attribute Based Encryption [MA-ABE] is used to overcome the drawbacks of the existing Patients health record system (PHR).

In this architecture, the EHR of the patients are stored in the server storage. It is the responsibility of the storage service provider for the storage and maintenance of the patients EHR. Since the data will be stored on the third party servers, security is of top concern. And to address this data security concern MA-ABE is used.

MA-ABE uses symmetric key cryptography for encrypting the data of the EHR. The EHR consists of several attributes such as patient, doctor, research and family friends, related to the health of the patient. Using MA-ABE, all the attributes or selected attributes of the EHR are encrypted using the secret key. The encryption increases the data security in the storage.

In this architecture, the users of the EHRs are divided into two domains namely, Professional domain and Non Professional domain. The Professional domain consists of Doctors, Research students who require data of the EHR for carrying out their professional activities. The Non Professional domain consists of the patient's relative and friends who require the data of the EHR for general usage.

The Multi Authority concept is used for abstracting the data from the EHR based on the user's authority. In multi authority technique, all the users are assigned an authority and based on this authority, data from the EHR is displayed to the user.

The proposed system fully realizes the patient-centric model by allowing the patient to manage his/her EHR. The patient can share his report with other doctors of different hospitals to get expert advice.

The proposed system also provides a very safe way for searching among the various EHRs by implementing the encrypted search. This technique encrypts the search string and then searches the encrypted record which reduces the risk of data compromise.

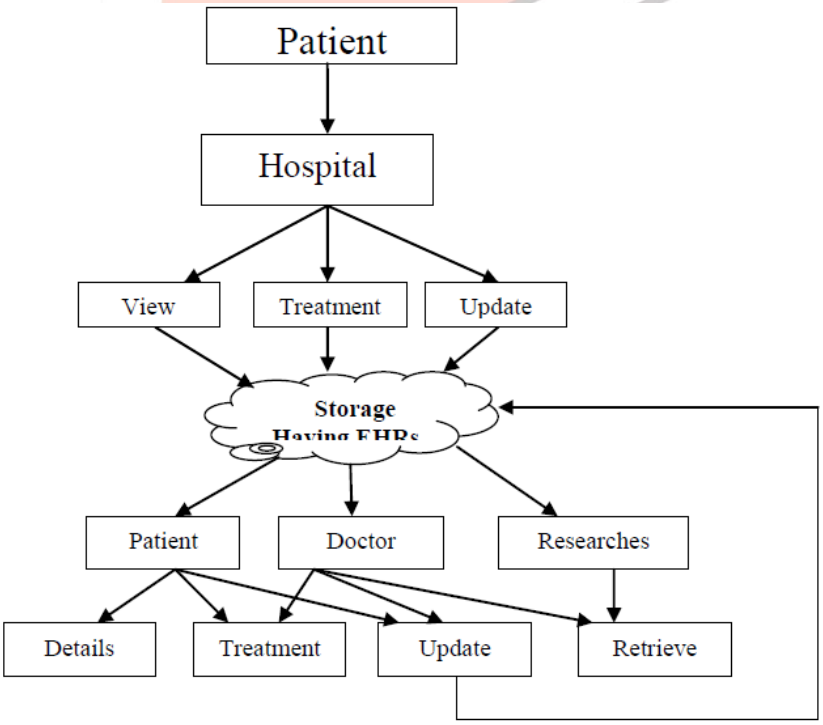

Fig 1 System Architecture

The System Architecture of proposed system is shown in Figure 1.when patient visits hospital his/her information will be documented by the hospital authorities. The user id and password will be provided to the patients to view the EHR status in their profile page. The patient's information reflected in the doctors profile page about patient details. The doctors have access rights to

update the treatment details and can share the EHR with hospital authorities in case of Emergency, the same updation will be reflected in the

Patient's page. Here EHR will be encrypted based on attributes. Hence professional domain user such as researchers and family friends can view only abstracted data and only doctors will be having write access to EHR and right to grant write permission, others can view only EHR data and as only hospital authorities have a right to grant awrite permission. When the same EHR shared with other hospitals, they can view the records but no alteration can be done in the EHR by the other hospital authorities.

For Example: A Patient named "X" admitted to hospital ABC in the month April, his/her records will be maintained in ABC hospital. If the same patient"X"admitted to some geographically distributed hospital say "IJK" in the month of june.he/she can provide a EHR of ABC hospital but IJK hospital authorities only can view EHR but to write EHR of patient they should get write permission from ABC hospital hence while sharing No hackers can alter the EHR as it will be encrypted based on attributes and also as EHR will be divided into segments or parts using Hiding Appropriate Message algorithm. while sharing. The receiver end will get a EHR in parts or segments. In worst case if the parts of EHR also hacked, as EHR will be internally encrypted using ABE algorithm, hence security will be preserved while sharing and privacy will be ensured at the same time.

IV. CONCLUSION

Multi Authority Attribute Based Encryption is a framework for Secure Sharing of Electronic Health Record. Healthcare users have complete control over their Electronic Health Records. As ABE method used, other users or roles such as researchers and family friends have access to view a abstracted information thus privacy ensured, While sharing EHR with other hospitals records will be encrypted using Hiding Appropriate Message algorithm. Hence first round of security will be provided. Later Internally encrypted using MA-ABE based on attributes so another round of security will be provided to ensure privacy and security.

V. ACKNOWLEDGEMENT

I take this Opportunity to express my profound gratitude and deep regards to my guide Prof. H R Shashidhar, Assistant Professor, RNS Institute of technology, Bangalore, for his exempla nary guidance, and constant encouragement throughout.

REFERENCES

[1] Arshdeep bahga and vijay madisetti, "a cloud based approach for interoperable electronic health records", 2013
[2] Daglish d, archer n. "electronic health record systems: a brief review of privacy security, and architectural issues "2011
[3] Leong chan, amer m, aldhaban f "adoption & evaluation of electronic health record (ehr) system"2011
[4] G. Ateniese, r. D. Pietro, l. V. Mancini, and. Tsudik "scalable and efficient provable data possession".2010
[5] OpenEHR, http://www.openehr.org, 2012.